UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MARGARET BIANUCCI, JIMMIE RAY HALE, JR., ANTONETTE HALL, KATHRYN EDWARDS, ERICA JUDKA, and FAITH SPIKER, individually and on behalf of all others similarly situated, Plaintiffs, v. RITE AID CORPORATION, Defendant.	Case No. 2:24-cv-03356 **CONSOLIDATED COMPLAINT – CLASS ACTION** JURY TRIAL DEMANDED

Plaintiffs Margaret Bianucci, Jimmie Ray Hale, Jr., Antonette Hall, Kathryn Edwards, Erica Judka, and Faith Spiker ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through the undersigned attorneys, bring this class action against Defendant Rite Aid Corporation, ("Rite Aid" or "Defendant") and complain and allege the following upon personal knowledge (as to their own actions) and an investigation by counsel, and information and belief as to all other matters.

INTRODUCTION

1. The release, disclosure, and publication of sensitive, personal information can be devastating. Not only is it an intrusion of privacy, but it is a harbinger of identity theft.

2. This class action arises out of a recent targeted cyberattack and data breach where unauthorized third-party criminals retrieved and exfiltrated the highly sensitive personal information of Plaintiffs and approximately 2.2 million similarly situated individuals from Rite Aid's computer network (the "Data Breach").

3. The personal information obtained during the Data Breach includes names, dates of birth, drivers' license numbers, and other forms of government issued IDs (collectively, "PII").

4. Defendant Rite Aid is a Philadelphia-based, Fortune 500 drugstore chain that operates more than 1,700 retail pharmacy locations across 16 states.[1] Rite Aid prides itself as a drug store chain with "lower healthcare costs through better coordination, stronger engagement, and personalized services that help you achieve whole health for life."[2]

5. During the regular course of conducting its daily business, Rite Aid acquires, collects, stores, and transfers its customers' PII. Rite Aid acquired Plaintiffs' and other similarly situated individuals' ("Class Members") PII while providing pharmacy and retail products and services.

6. Plaintiffs and Class Members are current and former customers of Rite Aid, who provided their sensitive PII to Rite Aid directly or indirectly in connection with Rite Aid's pharmacy and retail products and services.

7. On or about June 6, 2024, Rite Aid learned that "an unknown third party impersonated a company employee to compromise their business credentials and gain access to certain business systems."[3] Following an investigation of the breach, Rite Aid determined that "certain data associated with the purchase or attempted purchase of specific retail products was acquired by the unknown third party. This data included purchaser name, address, date of birth

---

[1] *Our Story*, Rite Aid, https://news.riteaid.com/about-us/history/default.aspx (last accessed Sept. 5, 2024).

[2] *Purpose, Values, and Mission*, Rite Aid, https://www.riteaid.com/about-us/mission-statement (last accessed Sept. 5, 2024).

[3] *Data Breach Notifications*, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/c4bace65-85df-4fff-b99f-f8fd390bb41a.html (last accessed Sept. 5, 2024).

and driver's license number or other form of government-issued ID presented at the time of a purchase between June 6, 2017, and July 30, 2018."[4]

8. Despite knowing of the Data Breach as early as June 6, 2024, Rite Aid did not begin sending notices to individuals affected by the Data Breach until mid-July. Plaintiffs were not notified of the Data Breach until Rite Aid began sending out Notice of Data Breach letters ("Notice") around July 15, 2024, well over one month after the Data Breach.

9. In its Notice, Rite Aid failed to provide important details about the Data Breach, including whether the cybercriminal(s) responsible for breach were identified or the information exfiltrated was held for ransom. Rite Aid also did not disclose whether its investigation detected compromised information on the dark web. Rite Aid simply offered credit monitoring and identity restoration services to affected individuals, but this offer is woefully inadequate, as it does not make Plaintiffs and Class Members whole for the harms caused by the Data Breach, nor does it protect them against the indefinite risk of harm caused by disclosure of their PII.

10. Rite Aid's Notice also did not disclose how it discovered the Data Breach, the means and mechanism of the cyberattack, and, importantly, what specific steps Rite Aid took following the Data Breach to secure its systems and prevent future cyberattacks.

11. Additionally, it appears that Rite Aid waited until after the notorious ransomware group RansomHub announced its targeted attack on the drugstore chain to acknowledge the cyberattack. RansomHub is a relatively new threat group that demands ransom payments from victims in exchange for not leaking stolen files, often auctioning the files to the highest bidder if negotiations fail. According to a post on RansomHub's leak site, the cybercriminal group obtained

[4] *Id*.

"over 10 GB of customer information equating to around 45 million lines of people's personal information."[5]

12. Because cyberattacks targeting large corporations are ubiquitous—in particular, attacks on entities like Rite Aid who straddle the healthcare industry—and in light of its prior May 2023 data breach,[6] it was foreseeable that Defendant would be the target of a cyberattack, and it should have taken appropriate precautions.

13. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect PII from the foreseeable threat of a cyberattack.

14. By being entrusted with Plaintiffs' and Class Members' PII for its own pecuniary benefit, Defendant assumed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to protect Plaintiffs' and Class Members' PII against unauthorized access and disclosure. Defendant also had a duty to adequately safeguard this PII under applicable law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"). Defendant breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices.

15. Cybercriminals can use or sell stolen PII to further harm Plaintiffs and Class

---

[5] Sergiu Gatlan, *Rite Aid confirms data breach after June ransomware attack*, BLEEPING COMPUTER (July 12, 2024), https://www.bleepingcomputer.com/news/security/rite-aid-confirms-data-breach-after-june-ransomware-attack/.

[6] In May 2023, Rite Aid announced that the PII and sensitive health data of 24,000 current and former customers was exfiltrated when a vulnerability in its systems was exploited by an unknown third party. *See* Mathis, Carlos, *Rite Aid customers' personal information accessed in data breach*, THE HILL (July 22, 2023), https://thehill.com/blogs/blog-briefing-room/4110730-rite-aid-customers-personal-information-accessed-in-data-breach/.

Members in a variety of ways including: destroying their credit by opening new financial accounts and taking out loans in Class Members' names; using Class Members' names to improperly obtain medical services; using Class Members' PII to target other phishing and hacking intrusions; using Class Members' PII to obtain government benefits; and otherwise assuming Class Members' identities.

16. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its systems were protected against unauthorized intrusions; failing to disclose that it did not have adequate practices and policies in place to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to train its staff and employees adequately on proper security measures; and failing to provide Plaintiffs and Class Members with prompt and adequate notice of the Data Breach.

17. Rite Aid's failure to notify the victims of its Data Breach in a timely manner meant that Plaintiffs and Class Members were unable to take quick action to prevent or mitigate the resulting harm.

18. Despite having been accessed and "acquired" by unauthorized criminal actors, Plaintiffs' and Class Members' sensitive and confidential PII remains in Defendant's possession. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

19. As a result of the Data Breach, Plaintiffs and approximately 2.2 million Class Members have suffered concrete harm and are now exposed to a heightened and imminent risk of fraud and identity theft for a period of years, if not decades. Furthermore, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiffs and the other Class Members will

incur ongoing out-of-pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

20. Plaintiffs and Class Members also will be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. Moreover, because the exposed information includes drivers' license numbers, government ID information, and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

21. Through this action, Plaintiffs, individually and on behalf of Class Members, seek to hold Defendant responsible for the harms caused by the Data Breach. Plaintiffs seek remedies for Defendant's negligence, negligence per se, breaches of fiduciary duty, unjust enrichment, breaches of implied contract, violations of state consumer protection statutes, and for declaratory and injunctive relief, including actual and statutory damages, restitution, and injunctive and declaratory relief; attorneys' fees, costs, and expenses incurred in bringing this action; and all other remedies the Court deems just and proper.

PARTIES

Plaintiffs

Plaintiff Margaret Bianucci

22. Plaintiff Margaret Bianucci is a resident and citizen of Pacheco, California. Plaintiff Bianucci's PII was provided to or obtained by Rite Aid in connection with its provision of its pharmacy and retail products and services.

23. Plaintiff Bianucci is careful about sharing her PII and takes reasonable steps to protect her PII. Plaintiff Bianucci has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff Bianucci stores any documents containing PII in a safe

and secure location and diligently chooses unique usernames and passwords for her online accounts.

24. At the time of the Data Breach, Rite Aid retained Plaintiff Bianucci's PII in its systems, and on information and belief it continues to retain that information.

25. Plaintiff Bianucci first learned of the Data Breach after receiving a notification letter from Rite Aid on or about July 15, 2024, notifying her of the Data Breach and that her PII had been improperly accessed and disclosed to unauthorized third parties. Upon receiving notice of the Data Breach, Plaintiff Bianucci made reasonable efforts to mitigate its impact, including, but not limited to, monitoring her various financial and banking accounts for fraudulent activity and fielding spam emails and calls daily.

26. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Bianucci will need to maintain these heightened measures for years.

27. In the time following the Data Breach, Plaintiff Bianucci has experienced an increase in spam emails and calls.

28. Plaintiff Bianucci also suffered actual injury from having her PII compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII—a form of property that was entrusted (indirectly) to Rite Aid and was compromised as a result of the Data Breach Rite Aid failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of her PII.

29. Plaintiff Bianucci has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Rite Aid disclosed her PII to unauthorized parties who may now use that information for improper and unlawful purposes.

30. Plaintiff Bianucci is exposed, and will continue to be exposed for the remainder of her life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her PII being obtained by unauthorized third parties and/or cybercriminals.

31. Plaintiff Bianucci is also at a continued risk of harm because, on information and belief, her PII remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

32. Plaintiff Bianucci has a continuing interest in ensuring that her PII, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff Jimmie Ray Hale, Jr.

33. Plaintiff Jimmie Ray Hale, Jr. is a resident and citizen of Apple Valley, California. Plaintiff Hale's PII was provided to or obtained by Rite Aid in connection with its provision of its pharmacy and retail products and services.

34. Plaintiff Hale is careful about sharing his PII and takes reasonable steps to protect his PII. Plaintiff Hale has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff Hale stores any documents containing PII in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

35. At the time of the Data Breach, Rite Aid retained Plaintiff Hale's PII in its systems, and on information and belief it continues to retain that information.

36. Plaintiff Hale first learned of the Data Breach after receiving a notification letter from Rite Aid in or around July 2024, notifying him of the Data Breach and that his PII had been

improperly accessed and disclosed to unauthorized third parties. Upon receiving notice of the Data Breach, Plaintiff Hale made reasonable efforts to mitigate its impact, including, but not limited to, verifying the legitimacy of the Notice of Data Breach, purchasing a VPN service, monitoring his various financial and banking accounts for fraudulent activity, and fielding spam emails and calls daily.

37. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Hale will need to maintain these heightened measures for years.

38. In the time following the Data Breach, Plaintiff Hale has experienced an increase in spam emails and phone calls.

39. Plaintiff Hale also suffered actual injury from having his PII compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII—a form of property that was entrusted (indirectly) to Rite Aid and was compromised as a result of the Data Breach Rite Aid failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of his PII.

40. Plaintiff Hale has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Rite Aid disclosed his PII to unauthorized parties who may now use that information for improper and unlawful purposes.

41. Plaintiff Hale is exposed, and will continue to be exposed for the remainder of his life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII being obtained by unauthorized third parties and/or cybercriminals.

42. Plaintiff Hale is also at a continued risk of harm because, on information and belief, his PII remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

43. Plaintiff Hale has a continuing interest in ensuring that his PII, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff Antonette Hall

44. Plaintiff Antonette Hall is a resident and citizen of Redmond, Washington. Plaintiff Hall's PII was provided to or obtained by Rite Aid in connection with its provision of its pharmacy and retail products and services.

45. Plaintiff Hall is careful about sharing her PII and takes reasonable steps to protect her PII. Plaintiff Hall has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff Hall stores any documents containing PII in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

46. At the time of the Data Breach, Rite Aid retained Plaintiff Hall's PII in its systems, and on information and belief continues to retain that information.

47. Plaintiff Hall first learned of the Data Breach after receiving a notification letter from Rite Aid on or about July 15, 2024, notifying her of the Data Breach and that her PII had been improperly accessed and disclosed to unauthorized third parties. Upon receiving notice of the Data Breach, Plaintiff Hall made reasonable efforts to mitigate its impact, including, but not limited to, monitoring her various financial and banking accounts for fraudulent activity and fielding spam emails and calls daily.

48. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Hall will need to maintain these heightened measures for years.

49. In the time following the Data Breach, Plaintiff Hall has experienced an increase in spam emails and calls.

50. Plaintiff Hall also suffered actual injury from having her PII compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII—a form of property that was entrusted (indirectly) to Rite Aid and was compromised as a result of the Data Breach Rite Aid failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of her PII.

51. Plaintiff Hall has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Rite Aid disclosed her PII to unauthorized parties who may now use that information for improper and unlawful purposes.

52. Plaintiff Hall is exposed, and will continue to be exposed for the remainder of her life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her PII being obtained by unauthorized third parties and/or cybercriminals.

53. Plaintiff Hall is also at a continued risk of harm because, on information and belief, her PII remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

54. Plaintiff Hall has a continuing interest in ensuring that her PII, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff Kathryn Edwards

55. Plaintiff Kathryn Edwards is a resident and citizen of Mount Vernon, Ohio. Plaintiff Edwards's PII was provided to or obtained by Rite Aid in connection with its provision of its pharmacy and retail products and services.

56. Plaintiff Edwards is careful about sharing her PII and takes reasonable steps to protect her PII. Plaintiff Edwards has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff Edwards stores any documents containing PII in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

57. At the time of the Data Breach, Rite Aid retained Plaintiff Edwards's PII in its systems, and on information and belief continues to retain that information.

58. Plaintiff Edwards first learned of the Data Breach after receiving a notification letter from Rite Aid on or about July 15, 2024, notifying her of the Data Breach and that her PII had been improperly accessed and disclosed to unauthorized third parties. Upon receiving notice of the Data Breach, Plaintiff Edwards made reasonable efforts to mitigate its impact, including, but not limited to, verifying the legitimacy of the Notice of Data Breach, monitoring her various financial and banking accounts for fraudulent activity, and fielding spam emails and calls daily.

59. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Edwards will need to maintain these heightened measures for years.

60. In the time following the Data Breach, Plaintiff Edwards has experienced an increase in spam emails and calls.

61. Plaintiff Edwards also suffered actual injury from having her PII compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII—a form of property that was entrusted (indirectly) to Rite Aid and was compromised as a result of the Data Breach Rite Aid failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of her PII.

62. Plaintiff Edwards has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Rite Aid disclosed her PII to unauthorized parties who may now use that information for improper and unlawful purposes.

63. Plaintiff Edwards is exposed, and will continue to be exposed for the remainder of her life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her PII being obtained by unauthorized third parties and/or cybercriminals.

64. Plaintiff Edwards is also at a continued risk of harm because, on information and belief, her PII remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

65. Plaintiff Edwards has a continuing interest in ensuring that her PII, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff Erica Judka

66. Plaintiff Erica Judka is a resident and citizen of Fogelsville, Pennsylvania. Plaintiff Judka's PII was provided to or obtained by Rite Aid in connection with its provision of its pharmacy and retail products and services.

67. Plaintiff Judka is careful about sharing her PII and takes reasonable steps to protect her PII. Plaintiff Judka has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff Judka stores any documents containing PII in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

68. At the time of the Data Breach, Rite Aid retained Plaintiff Judka's PII in its systems, and on information and belief continues to retain that information.

69. Plaintiff Judka first learned of the Data Breach after receiving a notification letter from Rite Aid on or about July 15, 2024, notifying her of the Data Breach and that her PII had been improperly accessed and disclosed to unauthorized third parties. Upon receiving notice of the Data Breach, Plaintiff Judka made reasonable efforts to mitigate its impact, including, but not limited to, monitoring her various financial and banking accounts for fraudulent activity, and fielding spam emails and calls daily.

70. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Judka will need to maintain these heightened measures for years.

71. In the time following the Data Breach, Plaintiff Judka has experienced an increase in spam emails and calls.

72. Plaintiff Judka also suffered actual injury from having her PII compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value

of Plaintiff's confidential PII—a form of property that was entrusted (indirectly) to Rite Aid and was compromised as a result of the Data Breach Rite Aid failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of her PII.

73. Plaintiff Judka has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Rite Aid disclosed her PII to unauthorized parties who may now use that information for improper and unlawful purposes.

74. Plaintiff Judka is exposed, and will continue to be exposed for the remainder of her life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her PII being obtained by unauthorized third parties and/or cybercriminals.

75. Plaintiff Judka is also at a continued risk of harm because, on information and belief, her PII remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

76. Plaintiff Judka has a continuing interest in ensuring that her PII, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff Faith Spiker

77. Plaintiff Faith Spiker is a resident and citizen of Palmerton, Pennsylvania. Plaintiff Spiker's PII was provided to or obtained by Rite Aid in connection with its provision of its pharmacy and retail products and services. More specifically, Spiker was required to provide her ID to be scanned every month when she picked up her prescriptions.

78. Plaintiff Spiker is careful about sharing her PII and takes reasonable steps to protect her PII. Plaintiff Spiker has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff Spiker stores any documents containing PII in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

79. At the time of the Data Breach, Rite Aid retained Plaintiff Spiker's PII in its systems, and on information and belief continues to retain that information.

80. Plaintiff Spiker first learned of the Data Breach after receiving a notification letter from Rite Aid on or about July 15, 2024, notifying her of the Data Breach and that her PII had been improperly accessed and disclosed to unauthorized third parties. Upon receiving notice of the Data Breach, Plaintiff Spiker made reasonable efforts to mitigate its impact, including, but not limited to, monitoring her various financial and banking accounts for fraudulent activity, and fielding spam emails and calls daily.

81. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Spiker will need to maintain these heightened measures for years.

82. In the time following the Data Breach, Plaintiff Spiker has experienced an increase in spam emails and calls.

83. Plaintiff Spiker also suffered actual injury from having her PII compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII—a form of property that was entrusted (indirectly) to Rite Aid and was compromised as a result of the Data Breach Rite Aid failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of her PII.

84. Plaintiff Spiker has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Rite Aid disclosed her PII to unauthorized parties who may now use that information for improper and unlawful purposes.

85. Plaintiff Spiker is exposed, and will continue to be exposed for the remainder of her life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her PII being obtained by unauthorized third parties and/or cybercriminals.

86. Plaintiff Spiker is also at a continued risk of harm because, on information and belief, her PII remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

87. Plaintiff Spiker has a continuing interest in ensuring that her PII, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Defendant

88. Defendant Rite Aid Corporation is a Delaware corporation with its principal place of business located at 1200 Intrepid Avenue, Second Floor, Philadelphia, Pennsylvania. It conducts business through several wholly-owned subsidiaries.

JURISDICTION AND VENUE

89. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because: (i) the amount in controversy exceeds $5 million, exclusive of interest and costs; (ii) the number of Class Members exceeds 100; and (iii)

minimal diversity exists because many Class Members, including Plaintiffs, have different citizenship from Defendant.

90. This Court has personal jurisdiction over Rite Aid because Rite Aid resides in and conducts substantial business in Pennsylvania and in this District through its principal place of business; engaged in the conduct at issue from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

91. Venue is proper under 28 U.S.C. § 1391(a) and (b) because Rite Aid's principal place of business is in this District and a substantial part of the events or omissions giving rise to the claims occurred in, were directed to, and/or emanated from this District.

GENERAL ALLEGATIONS

Overview of Rite Aid Corporation and Its Collection of PII

92. Founded in 1962 in Scranton, Pennsylvania, Rite Aid is a national drugstore chain based in Philadelphia. Rite Aid is headquartered in Penns Landing in Philadelphia, Pennsylvania.[7]

93. Rite Aid offers a range of retail products and services, including prescription drug services.

94. As a regular and necessary part of its business, Rite Aid collects and maintains sensitive PII from its customers, which it obtains and uses in connection with completing transactions. That information includes, but is not limited to, names, dates of birth, drivers' license numbers, and other government ID numbers. Rite Aid stores this information digitally.

[7] *Our History*, Rite Aid, https://www.riteaid.com/about-us/our-story (last accessed Sept. 5, 2024).

95. Rite Aid is and was aware of the sensitive nature of the PII it collects, and it acknowledges the importance of data privacy. Indeed, in its Privacy Policy on its website, Rite Aid claims that it "respects your concerns about privacy."[8]

96. The Privacy Policy goes on to state: "We maintain administrative, technical, and physical safeguards designed to protect personal information against accidental, unlawful, or unauthorized destruction, loss alteration, access, disclosure or use."[9]

97. Upon information and belief, Defendant promises its customers, including Plaintiffs and Class Members, to keep PII private; comply with healthcare drugstore industry standards related to data security and PII, including FTC guidelines; inform consumers of its legal duties and comply with all federal and state laws protecting consumer PII; only use and release PII for reasons that relate to the products and services Plaintiffs and Class Members obtain from Defendant; and provide adequate notice to individuals if their PII is disclosed without authorization. Based on its promises, Plaintiffs and Class Members reasonably expected that Rite Aid would do these things.

98. Defendant also promises that: "We will make any legally required disclosures of any breach of the security, confidentiality, or integrity of your personal information."[10] Plaintiffs and Class Members still have not received satisfactory information from Defendant concerning the Data Breach.

99. By obtaining, collecting, using, and benefitting from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties that required it to, at a minimum,

---

[8] *Privacy Policy*, Rite Aid, https://www.riteaid.com/legal/privacy-policy (last accessed Sept. 5, 2024).

[9] *Id*.

[10] *Id*.

implement adequate safeguards to prevent unauthorized use or disclosure of PII and to report any unauthorized use or disclosure of PII.

100. Contrary to Defendant's representations and assurances, it failed to implement adequate data security measures, as evidenced by Defendant's admission of the Data Breach.

The Data Breach

101. In data breach notification letters filed with the Office of Maine's Attorney General, Rite Aid disclosed that it detected the Data Breach on June 6, 2024, 12 hours after the attackers breached its network using an employee's credentials.[11]

102. Per these letters, Rite Aid "determined by June 17, 2024, that certain data associated with the purchase or attempted purchase of specific retail products was *acquired* by the unknown third party. This data included purchaser name, address, date of birth, and driver's license number or other form of government-issued ID presented at the time of a purchase between June 6, 2017, and July 30, 2018."[12]

103. Around July 15, 2024, Rite Aid began sending Plaintiffs and other Class Members the Data Breach Notice.

104. Omitted from the Notice was information explaining the root cause of the Data Breach or the vulnerabilities exploited by the cybercriminals. The Notice also makes no mention of the fact that Rite Aid was similarly targeted in a data breach in May 2023. To date, these omitted details have not been explained or revealed to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII is not repeatedly exposed to cybercriminals by Defendant.

[11] *Data Breach Notifications*, n. 3, *supra.*

[12] *Id*. (emphasis added).

105. Rite Aid's Notice also omits what computer systems were impacted, the means and mechanisms of the cyberattack, how it determined that the PII had been accessed, and (of particular importance to Plaintiffs and Class Members) the actual steps Rite Aid took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

106. Upon information and belief, the criminal ransomware gang RansomHub was involved in the Data Breach, and specifically targeted Defendant based on its status as a major drugstore with enormous amounts of valuable PII—including the PII of Plaintiffs and Class Members.

107. Because of the apparent involvement of a ransomware gang, Plaintiffs further believe that their and Class Members' PII has been or soon will be disseminated on the dark web, to be available for purchase. That is the *modus operandi* of cybercriminals, and the RansomHub gang has threatened exactly that: confirming in mid-July its intentions to leak Plaintiffs' and Class Members' PII that was exfiltrated from Rite Aid's insufficiently secured networks.[13]

108. Based on Rite Aid's acknowledgments, it is evident that unauthorized criminal actors did in fact access Rite Aid's network and exfiltrated Plaintiffs' and Class Members' PII in an attack designed to acquire that sensitive, confidential, and valuable information.

109. The PII contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have accessed Plaintiffs' and Class Members' PII.

110. As an entity that collects and maintains significant volumes of PII, the targeted attack was a foreseeable risk of which Rite Aid was aware and knew it had a duty to guard against.

[13] *See* n. 5, *supra.*

This is particularly true given that Rite Aid was the target of another cyberattack less than one year earlier.

111. The Data Breach reportedly impacted the PII of approximately 2.2 million individuals.

Rite Aid Failed to Follow FTC Guidelines

112. The Federal Trade Commission ("FTC") has regularly promulgated guidelines for businesses, which highlight the necessity of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

113. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[14]

114. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[15] The guidelines also recommend that businesses use an intrusion detection

[14] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[15] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (October 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

115. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

116. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.[16] Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

117. Rite Aid failed to properly implement the basic data security practices recommended by the FTC.

118. Defendant was at all times fully aware of its obligation to protect its customers' PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[16] *See*, *e.g. In the Matter of LabMD, Inc., A Corp*, No. 9357, 2016 WL 4128215, at *32 (F.T.C. July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act."), *vacated on other grounds, LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221 (11th Cir. 2018).

119. Rite Aid's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

Rite Aid Failed to Comply with Industry Standards for Data Security

120. In light of the evident threat of cyberattacks seeking consumers' PII, several best practices have been identified by regulatory agencies and experts that, at a minimum, should be implemented by companies within the healthcare industry, like Defendant, to secure Plaintiffs' and Class Members' PII.

121. Rite Aid is aware of the importance of safeguarding Plaintiffs' and Class Members' PII, and that by virtue of its business—as a company which operates a pharmacy—it placed Plaintiffs' and Class Members' PII at risk of being targeted by cybercriminals.

122. Because Rite Aid failed to implement, maintain, and comply with necessary cybersecurity requirements, it was unable to protect Plaintiffs' and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

123. Several best practices have been identified that, at a minimum, should be implemented by corporate entities like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, such as firewalls and anti-virus and anti-malware software; encryption (e.g., making data unreadable without a key); multi-factor authentication; backup data; and limiting the number of employees with access to sensitive data.

124. Other commonly accepted data security standards among businesses that store personal information, such as the PII involved here, include, but are not limited to:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for personal and financial information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

125. Defendant failed to meet the minimum standards of, e.g., the NIST Cybersecurity Framework, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established industry standards in reasonable cybersecurity readiness.

126. These foregoing frameworks are existing and applicable industry standards in the corporate sector and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

127. Despite Defendant's obligations, Defendant failed to appropriately monitor and maintain its data security systems in a meaningful way so as to prevent the Data Breach.

128. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

Rite Aid Owed a Duty to Safeguard PII, and It Breached That Duty

129. Rite Aid was aware of the importance of security in maintaining personal information (particularly sensitive personal information like the PII involved here), and the value consumers place on keeping their PII secure.

130. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiffs and Class Members.

131. Defendant owed a duty to Plaintiffs and Class Members, who entrusted Defendant with extremely sensitive PII to design, maintain, and test the information technology systems that housed Plaintiffs' and Class Members' PII, to ensure that the PII in Defendant's possession were adequately secured and protected.

132. Defendant owed a duty to Plaintiffs and Class Members to adequately train its employees and others with access to Plaintiffs' and Class Members' PII on the procedures and practices necessary to safeguard such sensitive information. This duty also required supervision, training, and compliance on Rite Aid's part to ensure that it complied with creating, implementing, and maintaining reasonable data security practices and procedures sufficient to protect Plaintiffs' and Class Members' PII.

133. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would enable Defendant to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

134. Defendant owed a duty to Plaintiffs and Class Members to disclose when and if its information technology systems and data security practices were not adequate to protect and safeguard Plaintiffs' and Class Members' PII.

135. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of inadequate data security practices.

136. Defendant violated these duties. Its Data Breach Notice states that Rite Aid became aware of the Data Breach on or about June 6, 2024, however, Plaintiffs, Class Members, and the public did not learn of the Data Breach until over a month later and did not know whether their PII was impacted until Rite Aid sent out the notice letters in July 2024. Defendant failed to publicly describe the full extent of the Data Breach and notify the affected parties. This demonstrates that Rite Aid did not properly implement measures designed to timely detect a data breach of their information technology systems, as required to adequately safeguard Plaintiffs' and Class Members' PII.

137. Rite Aid breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Rite Aid's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;
- Failing to adequately protect customers' PII;
- Failing to properly monitor its own data security systems for existing intrusions;
- Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- Failing to detect unauthorized ingress into its systems;
- Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;
- Failing to detect unauthorized exfiltration of the most sensitive data on its systems;

- Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;
- Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- Failing to adhere to industry standards for cybersecurity as discussed above; and
- Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' private PII.

138. Rite Aid negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cybercriminals to access its computer network, which contained unsecured and unencrypted PII.

139. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

140. However, due to Rite Aid's failures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Rite Aid.

The Data Breach Was a Foreseeable Risk, and Rite Aid Knew Criminals Target PII

141. The Data Breach was foreseeable and avoidable.

142. This Data Breach is not the only breach Defendant suffered in recent years. In May 2023, Defendant experienced another data breach which exposed the PII of over 24,000 individuals, including their sensitive personal health information like prescriptions and insurance details.[17]

[17] Lindsey O'Donnell-Welch, *Rite Aid Breach Stemmed from Compromised Credentials*, DECIPHER (July 16, 2024), https://duo.com/decipher/rite-aid-breach-impacts-2-2-million-customers.

143. Further, various governmental bodies have put entities like Defendant on notice of the likelihood of cyberattacks. In a Joint Cybersecurity Advisor, the Federal Bureau of Investigation ("FBI") and the Cybersecurity & Infrastructure Security Agency ("CISA") encouraged critical infrastructure organizations, such as Defendant, to implement their various recommendations as set forth in the advisory to reduce the likelihood and impact of inevitable ransomware and data extortion efforts, including against similar ransomware attacks perpetrated by similar ransomware gangs.[18]

144. Indeed, cyberattacks have been common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[19]

145. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[20]

---

[18] *See, e.g*, *#StopRansomware: ALPHV Blackcat*, AMERICA'S CYBER DEFENSE AGENCY (Feb. 27, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a; *#StopRansomware: ALPHV Blackcat*, AMERICA'S CYBER DEFENSE AGENCY (May 10, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a.

[19] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[20] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

146. The Office for Civil Rights ("OCR") also urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[21]

147. Moreover, in light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

148. Data breaches are preventable. As Lucy Thompson wrote in the *Data Breach and Encryption Handbook*, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[22] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…" and "[m]ost of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … [a]ppropriate

[21] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Department of Health and Human Services (Apr. 22, 2014), https://wayback.archiveit.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[22] Lucy L. Thompson, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2011) https://archive.org/details/isbn_9781604429893/page/28/mode/2up.

information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[23]

149. Additionally, as a HIPAA-covered entity handling PII, Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry, and other industries holding significant amounts of PII and personal health information, preceding the Data Breach. Although personal health information was not implicated in the instant Data Breach, Defendant's status as a pharmacy and therefore a HIPAA-covered entity should have put Defendant on high alert as to the importance of its data security obligations.

150. Healthcare-related breaches, in particular, have continued to rapidly increase because electronic patient data is seen as a valuable asset. In fact, entities that store patient information "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[24]

151. Healthcare entities suffered at least 337 data breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare data breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[25]

---

[23] *Id*.

[24] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXECUTIVE (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

[25] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, TECHTARGET (July 19, 2022),

152. According to the HIPAA Journal's 2023 Healthcare Data Breach Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[26]

153. Given the wealth of information from the law enforcement and healthcare industry concerning the increasing prevalence of cyberattacks, Defendant knew and should have known about its data security vulnerabilities and implemented enhanced and adequate protection to protect and secure Plaintiffs' and Class Members' Private Information. Even knowing the risk, Defendant failed to do so.

154. Defendant was well aware that the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to both the owners of the PII and those who would use it for wrongful purposes.

155. Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

156. Despite the prevalence of public announcements of data breach and data security compromises, and having already been the target of another data breach just one year prior, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

---

https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

[26] Steve Alder, *Security Breaches in Healthcare in 2023*, THE HIPAA JOURNAL (Jan. 31, 2024), www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf

157. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

158. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's servers, amounting to potentially hundreds of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

159. As a highly sophisticated party that handles sensitive PII, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII to protect against anticipated threats of intrusion of such information.

160. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

PII Is Inherently Valuable

161. PII is a valuable property right.[27] The value of PII as a commodity is measurable.[28] "Firms are now able to attain significant market valuations by employing business models

[27] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible..."), https://www.researchgate.net/publication/283668023.

[28] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

predicated on the successful use of personal data within the existing legal and regulatory frameworks."[29] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[30] Personal data is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

162. PII can sell for as much as $363 per record according to the Infosec Institute.[31] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

163. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to the criminal underworld.

164. There is an active and robust market for this information. As John Sancenito, president of Information Network Associates, a company which helps companies with recovery

---

[29] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220 at 4, OECD Publishing (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[30] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[31] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

165. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, driver's license numbers, other ID numbers, Social Security numbers, PII, and other sensitive information directly on various websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

166. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[32]

167. PII, like that stolen from Defendant, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[33]

[32] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[33] *See* n. 26, *supra.*

Plaintiffs and Class Members Suffered Harm as a Result of the Data Breach

168. Identity theft is the most common consequence of a data breach—it occurs to 65% of data breach victims.[34] Consumers lost more than $56 billion to identity theft and fraud in 2020, and over 75% of identity theft victims reported emotional distress.[35]

169. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[36]

170. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[37]

171. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, obtaining government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house, or receive medical

[34] Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE BLOG (Apr. 14, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics.

[35] *Id*.

[36] Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft

[37] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[38]

172. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[39]

173. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique known as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

---

[38] *Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Sept. 5, 2024).

[39] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

174. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use the information and trade it on dark web black-markets for years to come.

175. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

176. The PII exposed in the Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial.

177. Theft of drivers' license numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced.

178. Due to their highly sensitive nature, theft of drivers' license numbers in combination with other PII (e.g., name, address, date of birth) can result in a variety of fraudulent activity.

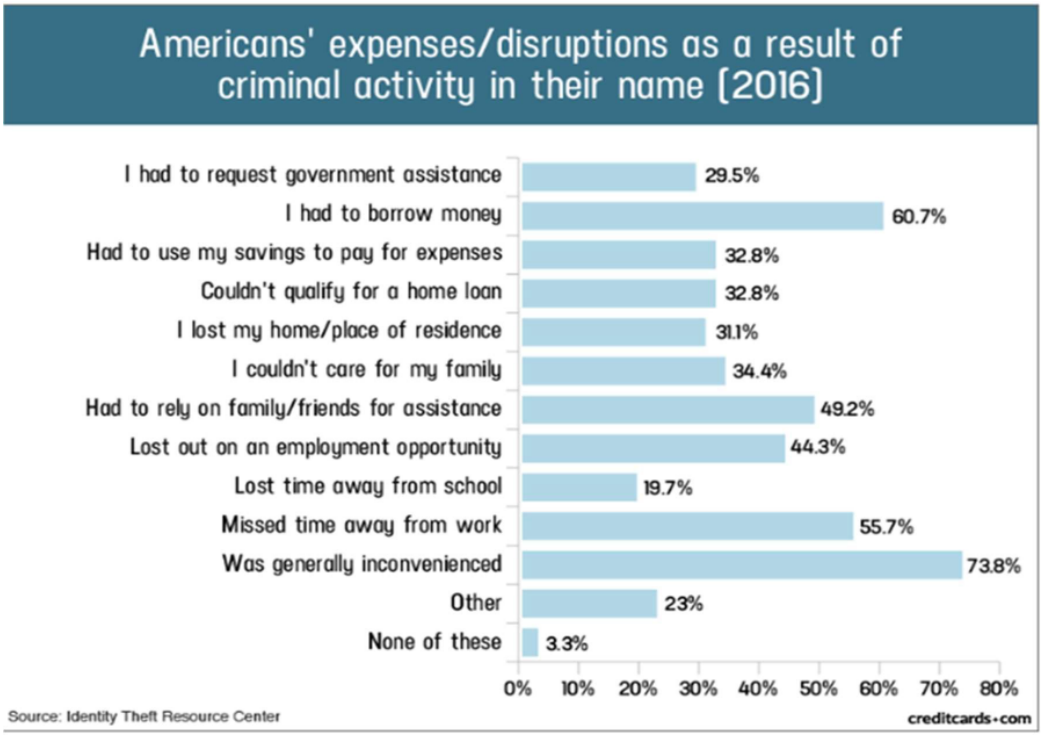
179. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected for weeks or months.

180. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[40]

[40] *Id.*

181. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



182. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

183. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[41] The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

[41] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

184. As a result of Rite Aid's conduct and failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII, which allowed the Data Breach to occur, Plaintiffs' and Class Members' PII has been and is now in the hands of unauthorized individuals and third parties, which may include thieves, unknown criminals, and other potentially hostile individuals.

185. Plaintiffs and Class Members greatly value their privacy, especially their PII. They would not have entrusted Rite Aid with their PII had they known that it would fail to adequately protect it. Indeed, Plaintiffs and Class Members provided Rite Aid with this highly sensitive information with the expectation that Rite Aid would keep their PII secure and inaccessible from unauthorized parties.

186. As a result of Rite Aid's failure to implement and follow even the most basic security procedures, Plaintiffs and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including, but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential PII used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' PII for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

187. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives.

188. Plaintiffs and Class Members are also at a continued risk of harm because their PII remains in Rite Aid's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Rite Aid fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

189. Plaintiffs and Class Members further face substantial risk of being targeted for phishing, data intrusion, and other illegal schemes based on Plaintiffs' and Class Members' PII, as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

190. Plaintiffs and Class Members further have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-

pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their names;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

191. As a result of the Data Breach, and in addition to the time Plaintiffs and Class Members have spent and anticipate spending to mitigate the impact of the Data Breach on their lives, Plaintiffs and Class Members have also suffered emotional distress from the public release of their PII, which they believed would be protected from unauthorized access and disclosure. The emotional distress they have experienced includes anxiety and stress resulting from the fear that unauthorized bad actors are viewing, selling, and or using their PII for the purposes of identity theft and fraud.

192. Additionally, Plaintiffs and Class Members have suffered damage to and diminution in the value of their highly sensitive and confidential PII —a form of property that Plaintiffs and Class Members entrusted to Rite Aid, and which was compromised as a result of the Data Breach Rite Aid failed to prevent. Plaintiffs and Class Members have also suffered a violation of their privacy rights as a result of Rite Aid's unauthorized disclosure of their PII.

193. Plaintiffs and Class Members were also damaged because they overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of their computer system(s) and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

194. To date, Defendant has done virtually nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach. Rite Aid offered credit monitoring, but did not disclose how it determined eligibility. Not only did Defendant fail to provide adequate ongoing credit monitoring or identity protection services for individuals impacted by the Data Breach, but the credit monitoring identity theft protection services does nothing to compensate Plaintiffs and Class Members for damages incurred, and time spent dealing with, the Data Breach.

195. Many failures laid the groundwork for the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cybersecurity training, procedures, and protocols that were necessary to protect Plaintiffs' and Class Members' PII.

196. Defendant maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

197. Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would result if Plaintiffs' and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of the breach.

198. The risk of improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' PII from that risk left the PII in a dangerous condition.

199. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members with prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

200. Plaintiffs bring this case individually and, pursuant to Rule 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on behalf of the following Nationwide Class and State Classes (collectively the "Class"):

> **Nationwide Class**
> All residents of the United States whose PII was compromised in the Rite Aid Data Breach, including all persons who received notice of the Data Breach.

In addition, or in the alternative, Plaintiffs propose the following state classes:

> **California Class**
> All residents of California whose PII was compromised in the Rite Aid Data Breach, including all persons who received notice of the Data Breach.
>
> **Washington Class**
> All residents of Washington whose PII was compromised in the Rite Aid Data Breach, including all persons who received notice of the Data Breach.

Ohio Class
All residents of Ohio whose PII was compromised in the Rite Aid Data Breach, including all persons who received notice of the Data Breach.

Pennsylvania Class
All residents of Pennsylvania whose PII was compromised in the Rite Aid Data Breach, including all persons who received notice of the Data Breach.

201. Excluded from the Class is Rite Aid, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Rite Aid has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

202. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

203. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. As noted above, there are approximately 2.2 million Class Members.

204. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including, but not limited to, the information implicated in the Data Breach.

205. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions

of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to secure and protect the PII of Plaintiffs and Class Members;

b. Whether Defendant was negligent in collecting and disclosing Plaintiffs' and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiffs' and Class Members' PII in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

j. Whether Plaintiffs and Class Members are entitled to declaratory judgment under 28 U.S.C. § 2201, *et seq.*;

k. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conducts; and

l. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

206. The requirements of Rule 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of Class Members. The claims of the Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiffs and Class Members each had their PII disclosed by Defendant to an unauthorized third party.

207. The requirements of Rule 23(a)(4) are satisfied. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class Members. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation, including data breach litigation. The claims of Plaintiffs and Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation

method available to Plaintiffs and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class Member.

208. Here a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go unremedied.

209. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant's data security practices were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

210. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to the names and addresses of Class Members affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

211. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

212. Plaintiffs plead this claim on behalf of the Nationwide Class or, alternatively, on behalf of the State Classes under the laws of those states.

213. Rite Aid owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

214. Rite Aid knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class Members' PII and the importance of maintaining secure systems. Rite Aid knew, or should have known, of the vast uptick in data breaches in recent years. Rite Aid had a duty to protect the PII of Plaintiffs and Class Members.

215. Given the nature of Rite Aid's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Rite Aid should have identified the vulnerabilities to

its systems and prevented the Data Breach from occurring, which Rite Aid had a duty to prevent.

216. Rite Aid breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the PII entrusted to them—including Plaintiffs' and Class Members' PII.

217. It was reasonably foreseeable to Rite Aid that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PII to unauthorized individuals.

218. But for Rite Aid's negligent conduct/breach of the above-described duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

219. As a result of Rite Aid's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation and diminution in the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the

effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II

NEGLIGENCE PER SE

(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

220. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

221. Plaintiffs plead this claim on behalf of the Nationwide Class or, alternatively, on behalf of the State Classes under the laws of those states.

222. In addition to the common law, Rite Aid's duties arise from Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Rite Aid, of failing to employ reasonable measures to protect and secure PII.

223. Rite Aid violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and all other Class Members' PII and not complying with applicable industry standards. Rite Aid's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

224. Rite Aid's violations of Section 5 of the FTC Act constitutes negligence per se.

225. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTC Act was intended to protect.

226. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTC Act was intended to guard against.

227. It was reasonably foreseeable to Rite Aid that its failure to exercise reasonable care

in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' PII to unauthorized individuals.

228. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Rite Aid's violations of Section 5 of the FTC Act. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation and diminution in the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III

BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

229. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

230. Plaintiffs plead this claim on behalf of the Nationwide Class or, alternatively, on behalf of the State Classes under the laws of those states.

231. Plaintiffs and Class Members either directly or indirectly gave Rite Aid their PII in confidence, believing that Rite Aid—a healthcare organization—would protect that information.

Plaintiffs and Class Members would not have provided Rite Aid with this information had they known it would not be adequately protected. Rite Aid's acceptance and storage of Plaintiffs' and Class Members' PII created a fiduciary relationship between Defendant and Plaintiffs and Class Members. In light of this relationship, Rite Aid must act primarily for the benefit of its patients (at least insofar as it relates to the safeguarding of their PII).

232. Rite Aid has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII, failing to comply with the data security guidelines set forth by Section 5 of the FTC Act, and otherwise failing to safeguard the PII of Plaintiffs and Class Members it collected.

233. As a direct and proximate result of Rite Aid's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Rite Aid's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV

UNJUST ENRICHMENT

(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

234. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

235. Plaintiffs plead this claim on behalf of the Nationwide Class or, alternatively, on behalf of the State Classes under the laws of those states.

236. This claim is pleaded in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d)(2).

237. Plaintiffs and Class Members conferred a monetary benefit upon Rite Aid in the form of monies paid for educational services or other services.

238. Rite Aid accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Rite Aid also benefited from the receipt of Plaintiffs' and Class Members' PII.

239. As a result of Rite Aid's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

240. Rite Aid should not be permitted to retain the money belonging to Plaintiffs and Class Members because Rite Aid failed to adequately implement the data privacy and security procedures for themselves that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, local laws, and industry standards.

241. Rite Aid should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

242. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

243. Plaintiffs plead this claim on behalf of the Nationwide Class or, alternatively, on behalf of the State Classes under the laws of those states.

244. Defendant required Plaintiffs and Class Members to provide, or authorize the transfer of, their PII in order for Rite Aid to provide healthcare services. In exchange, Rite Aid entered into implied contracts with Plaintiffs and Class Members in which Rite Aid agreed to comply with their statutory and common law duties to protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

245. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

246. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

247. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

248. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of their implied contracts with Plaintiffs and Class Members.

COUNT VI

VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018
Cal. Civ. Code §§ 1798.100 *et seq*. ("CCPA")

(On Behalf of Plaintiffs Bianucci and Hale and the California Class)

249. Plaintiffs Margaret Bianucci and Jimmie Ray Hale, Jr. ("Plaintiffs," for the purposes of this count) reallege and incorporate all previous allegations as though fully set forth herein.

250. Plaintiffs bring this claim on behalf of themselves and the California Class.

251. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

252. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

253. Rite Aid is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

254. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for"

statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

255. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because he/she is natural person residing in the State of California.

256. Rite Aid is a "business" as defined by Civ. Code § 1798.140(c).

257. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual." See Civ. Code § 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).

258. Plaintiffs' PII compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

259. Through the Data Breach, Plaintiffs' PII was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format

260. The Data Breach occurred as a result of Rite Aid's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

261. Plaintiffs Bianucci and Hale sent notice to Defendant pursuant to Cal. Civ. Code § 1798.150(b)(1) on July 25, 2024 and August 7, 2024, respectively. Because 30 days have lapsed without a response, Plaintiffs are seeking actual and/or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A), with respect to Plaintiffs Bianucci and Hale only.

262. As a result of Rite Aid's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs Bianucci and Hale seek statutory damages of up to $750 per class member (and no less than $100 per class member), actual damages to the extent they exceed statutory damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VII

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. and Prof. Code §§ 17200, *et seq*. ("UCL")
(On Behalf of Plaintiffs Bianucci and Hale and the California Class)

263. Plaintiffs Margaret Bianucci and Jimmie Ray Hale, Jr. ("Plaintiffs," for the purposes of this count) reallege and incorporate by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

264. Plaintiffs bring this claim on behalf of themselves and the California Class.

265. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

266. By reason of Defendant's above-described wrongful actions, inaction, and omission, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs' and Class Members' PII, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

267. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the private and confidential PII of consumers has been compromised for all to see, use, or otherwise exploit.

268. Defendant's practices were unlawful and in violation of the CCPA and CLRA and Defendant's own privacy policy because Rite Aid failed to take reasonable measures to protect Plaintiffs' and Class Members' PII.

269. Defendant's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII they provide to Defendant will remain private and secure, when in fact it was not private and secure.

270. Plaintiffs and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII.

271. Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 *et seq*., in that Defendant's conduct was substantially injurious to Plaintiffs and Class Members, offensive to public policy, immoral, unethical, oppressive, and unscrupulous, and the gravity of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

272. But for Defendant's misrepresentations and omissions, Plaintiffs and Class Members would not have provided their PII to Defendant, or would have insisted that their PII be more securely protected.

273. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs and Class Members' PII, they have been injured as follows: (1) the loss of the opportunity

to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendant; (3) the increased, imminent risk of fraud and identity theft; (4) the compromise, publication, and/or theft of their PII; and (5) the costs associated with monitoring their PII, amongst other things.

274. Plaintiffs take upon themselves enforcement of the laws violated by Defendant in connection with the reckless and negligent disclosure of PII. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiffs by forcing them to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

COUNT VIII

VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.* ("CCRA")
(On Behalf of Plaintiffs Bianucci and Hale and the California Class)

275. Plaintiffs Margaret Bianucci and Jimmie Ray Hale, Jr. ("Plaintiffs," for the purposes of this count) reallege and incorporate by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

276. Plaintiffs bring this claim on behalf of themselves and the California Class.

277. The California legislature enacted Cal. Civ. Code § 1798.81.5 "to ensure that Personal Information about California residents is protected."

278. The CCRA requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

279. Defendant is a business that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs and California Class Members.

280. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired, or is reasonably believed to have been acquired, by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

281. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

282. Plaintiffs and the California Class Members' PII includes Personal Information as covered by Cal. Civ. Code § 1798.82.

283. Because Defendant reasonably believed that Plaintiffs' and California Class Members' PII was acquired by unauthorized third parties during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion in accordance with Cal. Civ. Code § 1798.82.

284. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

285. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Class Members suffered damages, as described herein.

286. Plaintiffs and California Class Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT IX

VIOLATIONS OF THE WASHINGTON CONSUMER PROTECTION ACT RCW §§ 19.86.010 *et seq*. ("WCPA")

(On Behalf of Plaintiff Hall and the Washington Class)

287. Plaintiff Antonette Hall ("Plaintiff," for the purposes of this count) realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

288. Plaintiff Hall brings this claim on behalf of the Washington Class.

289. Plaintiff and Defendant are "persons" under the WCPA. RCW § 19.86.010(1).

290. Defendant's sale of pharmaceutical and retail products and services to Plaintiff and Washington Class Members constitutes as "trade" and "commerce" under the WCPA. RCW § 19.86.010(2).

291. The WCPA states, "Unfair methods of competition and unfair or deceptive practices in the conduct of any trade or commerce are hereby declared unlawful." RCW § 19.86.020. Defendant's sale of pharmaceutical and retail products and services to Plaintiff Hall and the Washington Class Members is an "unfair or deceptive practice" under the WCPA.

292. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

293. Pursuant to RCW § 19.86.090, Plaintiff Hall seeks actual damages and treble damages of up to three times the amount of actual damages on behalf of herself and Washington Class Members.

294. Plaintiff also seeks equitable relief, including an injunction, as the court deems necessary and proper.

295. Pursuant to RCW § 19.86.095, a copy of this Complaint will be served upon the Washington Attorney General.

COUNT X

VIOLATION OF THE OHIO CONSUMER SALES PRACTICES ACT
ORC §§ 1345, *et seq.*
(On Behalf of Plaintiff Kathryn Edwards and the Ohio Class)

296. Plaintiff Kathryn Edwards ("Plaintiff," for the purposes of this count) realleges and incorporates by reference each and every allegation contained elsewhere in this Complaint as if fully set forth herein.

297. Plaintiff brings this claim on behalf of herself and the Ohio Class.

298. Plaintiff and Ohio Class Members are "consumers" as defined by ORC § 1345.01(D).

299. Rite Aid advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

300. Rite Aid engaged in unfair and deceptive acts and practices in the conduct of a consumer transaction, in violation of ORC § 1345.02 and unconscionable consumer sales acts and practices in violation of ORC § 1345.03, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Ohio Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio Class Members' PII, including duties imposed

by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with Ohio's Data Security Act, ORC § 1354, which provides an affirmative defense to any cause of action in tort brought under Ohio law for failure to implement reasonable information security controls resulting in a data breach involving personal or restricted information. ORC § 1354.02(D)(2).

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Ohio Class Members' PII, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Ohio Class Members' PII; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

301. Rite Aid's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Rite Aid's data security and ability to protect the confidentiality of consumers' PII.

302. Had Rite Aid disclosed to Plaintiff and Ohio Class Members that its data systems were not secure and thus vulnerable to attack, Rite Aid would have been forced to adopt reasonable

data security measures and comply with the law. Rite Aid was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Ohio Class. Rite Aid accepted the responsibility of protecting the data, while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Ohio Class Members acted reasonably in relying on Rite Aid's misrepresentations and omissions, the truth of which they could not have discovered.

303. As a direct and proximate result of Rite Aid's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Ohio Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including, but not limited to, one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of PII; lost value of access to PII permitted by Rite Aid; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Rite Aid's Data Breach; lost benefits of bargains as well as overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

304. Plaintiff and Ohio Class Members seek all monetary and non-monetary relief allowed by law, including actual damages under ORC § 1345.09(A); declaratory and injunctive relief under ORC § 1345.09(D); reasonable attorneys' fees and costs, under ORC § 1345.09(F); and any other relief that is just and proper.

PRAYER FOR RELIEF

Plaintiffs, individually, and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Rite Aid as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, individually, and on behalf of the Class, seek appropriate injunctive relief designed to prevent Rite Aid from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft.

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 16, 2024

Respectfully submitted,

/s/ Andrew W. Ferich
Andrew W. Ferich (PA Bar 313696)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Benjamin F. Johns (PA Bar 201373)
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
Facsimile: (856) 210-9088
bjohns@shublawyers.com

Ashley M. Crooks (admitted *pro hac vice*)
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
acrooks@hausfeld.com

Kevin Laukaitis (*pro hac vice forthcoming*)
LAUKAITIS LAW LLC
954 Avenida Ponce Dr Leon, Suite 205 #10518
San Juan, PR 00907
Telephone: (215) 789-4462
klaukaitis@laukaitislaw.com

Thomas E. Loeser (*pro hac vice forthcoming*)
COTCHETT PITRE & MCCARTHY LLP
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Telephone: (206) 802-1272
Facsimile: (650) 697-0577
tloeser@cpmlegal.com

Interim Co-Lead Counsel for Plaintiffs and the Proposed Classes